An Evaluation Of The Comprehensibility and Usability Of a Design Method For Ubiquitous Computing Applications

Technical Report

Giovanni Iachello, Gregory Abowd

College of Computing and GVU Center

Georgia Institute of Technology

August 17, 2005

Abstract

We have recently proposed a design process framework that assists the practitioner in tackling the privacy and security issues of ubiquitous computing (ubicomp) applications during their development. In this report, we discuss a design study to evaluate the comprehensibility and usability of the design method. The study was conducted with six graduate students at our institution. Students were given the option of using the design method for completing a semester-long design exercise of a ubiquitous computing application of their choice. Researchers analyzed their written deliverables using quantitative metrics and conducted follow-up interviews. Results suggest that the design method is comprehensible and usable by inexperienced designers. Participants commented that the method might help especially in the design of exploratory applications with diverging stakeholders, broadening the coverage of the design process and generating stronger rationales for design decisions.

Keywords

Design Methods; Evaluation; Ubiquitous Computing; Security; Privacy; Requirements Engineering;

Introduction

We have recently proposed a design process framework that assists practitioners in making reasoned and documented design choices in the design of ubiquitous computing applications with privacy and security implications [7]. This design method is called hereafter the *proportionality* method because it is based on the principle of proportionality used in the legal and data protection communities in reference to privacy and technology.

We have applied the proportionality method to some case studies of ubicomp applications developed by our research group. In a first case study, we used the proportionality method to analyze the design of a potentially contentious application, and to plan its user evaluation. The results of this exercise, documented in [7], suggest that the design method may have contributed to a high-quality design of the user interface and information policies and improved understanding of the uses and risks associated with the application, along with the corrective measures necessary during its deployment.

Based on this experience, we claim that the design method may increase the coverage of security and privacy requirements analysis and improve design quality. In order to understand whether the design method is actually usable by others, we tested the method with external designers. This paper describes this test, which involved six graduate volunteer students in the Information Security Strategy class held at our institution during the Spring 2005 semester.

Related Work

Privacy and Security are significant concerns in the ubicomp community, raised both by researchers [13] and non-technical observers [10]. Over the past few years there have been several attempts to provide design guidelines for the development of privacy-respecting ubicomp applications, *e.g.*, Langheinrich's application of some of the Fair Information Practices (FIPS) [12] to ubicomp design [9] and Jiang *et al.*'s proposal of using economic and information theories to modulate flows of personal data in these systems [8].

However, there are very few proposals for systematic design approaches or methods. Bellotti and Sellen have proposed a design framework for multimedia awareness applications (*e.g.* video teleconferencing) based on feedback and control [1]. Hong *et al.* proposed to use a structured risk analysis process to aid the design of these applications, but have not evaluated their method [5, 6].

To the best of our knowledge, the only design method that has been evaluated in this domain is Chung *et al.*'s set of design patterns for ubicomp design [2]. They propose the use of design patterns, developed through iterative refinement with the help of several teams of designers who tested the patterns in a design study. Among other patterns, they also include 15 patterns specifically aimed at the privacy issues in ubicomp. However, they report that their participants did not use the privacy-specific design patterns in any meaningful way to complete the design exercises that were proposed. According to the researchers, the probable causes of this are that the proposed patterns were too abstract, that privacy issues were not emphasized enough in the design exercises' briefs, and in general that patterns might not be suited for addressing non-functional requirements such as privacy.

To cater to the non-functional nature of privacy and security requirements, our design suggestions focus on design process rather than specific solutions exemplified by patterns. We also believe that evaluating the method's performance is fundamental to understanding whether the proposed method is usable by the intended target group, and if, and in what circumstances, it is useful.

Process

The objective of this study was that of verifying the following two theses:

1. The proportionality method is understandable to and usable by inexperienced designers.
2. Inexperienced designers reach similar conclusions as experienced designers. The hypothesis is that they would identify the same main design issues and reach similar conclusions on these issues as the expert designers.

We recruited three groups (of two students each) of volunteer Master's students in the Information Security Strategy class at our institution to perform a design exercise using the proportionality method as a semester-long design assignment. Recruitment was made by sending emails of the descriptions of two projects to the whole class, prior to a lecture in which the recruitment would be made.

During this lecture, the researchers introduced the general domain of ubicomp, its security and privacy challenges, described design method and relevant bibliographic and legislative resources. Project goals were to design (but not implement) their choice between two ubicomp applications with known privacy and security issues. Participating students were asked to take on, as their main semester-long assignments one of these projects instead of other projects offered by the instructors of the class or projects that the student proposed him/herself. We asked volunteer participants to form groups of two. We chose to have small groups instead of individuals participate due to the potentially complex and unfamiliar problem domain and large amount of effort necessary to complete the assignments.

The first proposed application consisted in a mobile person finder running on a cell phone. This application allows users to ask the location of others and respond to location requests. The application supports users in meeting up, either in person or per phone, assessing the availability of the other persons,

or coordinating joint activities. The project brief stressed the use of the tool for *personal* use, as opposed to location systems for commercial settings such as logistics and trucking. Students were provided some references to relevant resources, including existing systems such as AT&T Find People Nearby and legislation regulating location-enhanced wireless services.

The second application we offered consisted in a system that records behavioral data of a child in an educational primary school setting (including audio and video). The system's purpose is to support teachers and other school personnel in recording observations about a child before, during and after critical incidents (e.g. escaping the classroom, temper tantrum). This system is loosely inspired by a system currently being designed by members of our research group [4].

Each group was asked to design (not to implement) the information management, organizational policies and privacy- and security-sensitive aspects of the user interface of a system to support the respective application. The groups were asked to justify their technical and organizational design choices and to reference legislation, local regulation, and other policies as appropriate. In addition, they were encouraged to follow the proportionality design method for the analysis of security and privacy requirements. Use of the design method was not mandatory, however. Participants were asked to justify their choice if they opted not to use the method.

At the beginning of the study, each participant signed consent forms and completed a questionnaire assessing their experience with requirements engineering techniques, information security standards, IT legislation and the ubicomp domain.

Participants had roughly two months to complete the assignment. After one month, each group was asked to make a short presentation (20 minutes) in class about their project progress. They also turned in an intermediate report (*mid-project milestone*), which was neither graded nor analyzed but helped insure that students would be on track with the assignment. The mid-term presentation and deliverables had to include an initial review of design options, list relevant literature, legislative and other resources, and identify all stakeholders of the application. During their presentation, students also received feedback by other students in the class, by the instructor and by one researcher.

At the end of the second month, all groups turned in a final deliverable in which they were asked to include at least the discussion of the following items:

- Regulatory constraints.
- Experience from similar applications.
- Description of system design.
- Discussion of the selected design for the system.
    - Information management policies.
    - Technical safeguards for securing data and people, including relevant aspects of the user interface (*e.g.*, how the system is operated, accessed, *etc.*)
- Organizational measures to be adopted contextually with system use.

We evaluated the design products, by comparing the design documents produced by the students with similar designs produced by an expert designer (one of the researchers).

After the end of the course, we interviewed participants to understand how they had used the proportionality method. This semi-structured interview included questions pertaining to:

- The understandability of the description of the design method (which consisted in a previous published paper [7]);

– The application of the design method (including a subjective assessment of time required to complete the assignment[1] and the impact on the quality of the end product);

– The resources they had accessed during the design, and feedback on specific design choices.

The interview lasted between 30 and 45 minutes and was conducted one group at the time. The participation in the interview was voluntary and separate from the rest of the study (all participants chose to take part in the interview). Since the interview did not provide credit for the class curriculum, each participant received a USD10 gift card as a token for participation.

Results

Clearly, with this study we did not intend to obtain statistically significant data. Rather, our objective was that of pointing out potential benefits of the design method and aspects needy of improvement.

Demographics

Participants did not have professional experience in ubicomp design. Some participants in groups 1 and 3 had some professional experience with information security issues. All participants were students of the Information Security MS program at Georgia Tech. Most participants had a technical background, except for one participant in group 3, who had a technology policy background.

Analysis

We identified 10 quantitative metrics to evaluate the completeness of the written final reports (we did not consider the oral presentations in this analysis). These metrics are based on the number of occurrences of the following *analysis elements*:

– expressed threats;

– usage scenarios;

– comparisons with existing similar applications;

– identified stakeholders;

– stated requirements;

– stated design choices;

– open design issues (that is, design points that were raised by the participants but no conclusion was reached, pending more information or the verification of some other hypothesis);

– architectural components of the design;

– specific items of legislation referenced;

– indications of the need for extended evaluations (*e.g.*, further surveys, interviews, *etc.*).

The first four metrics were selected to measure the thoroughness of the analysis performed by the participants. The following four metrics measure the complexity of the resulting design. Finally, the last two metrics reference external resources that had become necessary during the design process (*i.e.*, stakeholders' opinions, legislation, *etc.*).

We counted the occurrence of each type of metric by analyzing each statement or paragraph in the written reports. Guidance provided to the participants suggested a specific organization of their reports. However, only groups 2 and 3 loosely followed these suggestions. For this reason, the identification of countable

[1] The interview was performed after they had received a grade for the assignment. The researchers did not grade the assignment.

occurrences of the analysis elements is not as rigorous as would be desirable. In many cases, elements were not explicit and had to be extrapolated. The table below synthesizes these results. In all three groups' reports, the report size (in number of paragraphs) is roughly proportional to the sum of all analysis elements.

The numbers in the table should be taken at face value and not compared across columns because they are the result of different analysis processes without any control on the amount of time used in the analysis. In addition, these bare numbers do not tell whether the identified analysis elements were pertinent to the specific analysis. To control this variable, we further examined each design choice made by the three groups to assess whether it had a strong impact on stakeholder privacy or security.

Table 1 Deliverables Coverage At A Glance

	Group 1	**Group 2**	**Reference**	**Group 3**	**Reference**
Application	Person Finder	Person Finder	Person Finder	Video Recording	Video Recording
Used Method	No	Yes	Yes	Yes	No
Analysis Elements					
Threats	0	3	3	13	5
Scenarios	0	3	0	0	0
Comparisons with Similar Apps	2	0	2	2	7
Stakeholders	(1)[2]	2	3	7	5
Requirements	12	5	5	9	12
Design Choices	8	11	11	15	13
↳ Of which relevant to privacy / security	↳ 6	↳ 6	↳ 11	↳ 13	↳ 13
Open Design Issues	4	6	2	7	2
Architectural Components	4	4	1	5	NA
Legislation	2	4	2	2	3
Extended Evaluation	0	0	3	3	NA
TOTAL	33	38	31	63	47
Report Size[3]	98	102	106	197	145

Discussion

All three groups provided strong evidence of having understood the method's core concepts well enough to use the method or to make a justified decision not to use it. Group 1 did not use the design method, claiming that the existence of very similar commercial applications voided the need for applying a detailed design method. Both group members had a technical background and started the analysis from a feasibility assessment. They based their analysis on the comparison with two other similar applications.

[2] The number of stakeholders was not indicated explicitly.
[3] Report size is expressed in number of paragraphs in the document.

The comparison process, in their words, “jumpstarted” the design process and “gave a feel for what’s possible.”

Group 2 did use the design method but skipped the first phase (which requires to balance application usefulness with stakeholder privacy concerns), because these “requirements were already given” and they “did not feel necessary to justify that the application was useful”. The existence of similar services on the market might have influenced this assessment.

Group 3 stated that they applied a cyclic design process to discover design issues and decide upon them, as suggested by the proportionality method. The other two groups used a top-down type of design, in which broad architectural decisions were followed by detailed design.

The groups using the design method provided evidence of engaging in more elaborate—and more time-consuming—evaluation of alternative design options, relying less on existing applications’ critique. This fact is reflected in part by the numbers in the table. Participants in group 1 concentrated their analysis on the user interface of the application, specifying its design (hence the high number of Requirements). The same group did not spend as much effort in identifying threats to stakeholders’ privacy.

All participants who used the design method agreed that the application of the method had not increased the design time by itself, but they also indicated that they were induced to explore more design alternatives, and with greater depth, which required increased effort and time. Group participants that used the method commented in the interviews that their designs were more thorough because of this than they would have otherwise been.

This was reflected by the completeness of the design documentation provided by the three groups. The group that did not use the method explored only one technological solution, mainly basing their design on a comparison with, and enhancement of, similar existing services, whereas the groups that did use the design method generated more detailed designs. The groups that used the design method identified a higher number of design issues (summing open design issues and design choices) than the group that did not.

One member of one of the groups which used the design method stated that the hardest part in its application concerned the balancing of application usefulness with the risks on stakeholder privacy and that “the hard part was playing both roles [involved in the balancing].” The balancing of cost-effectiveness, usefulness and privacy was also cited by one participant as a challenging, but useful exercise. In particular, the participant indicated that this process help him in reaching decisions among alternative design options with privacy implications.

Finally, one group indicated that initially the application of the method had seemed “silly and redundant” but that eventually, the output of the analysis process, especially the documented evaluation of several alternative technical solutions, had been very useful as a *communication tool*. This group had talked about their design with potential stakeholders (two individuals with professional experience in education) and had found that the design output had been handy to justify and describe a particular solution in that context. Participants in one group commented that the design method would be most appropriate for exploratory applications, and less so for established technologies.

Regarding the similarity of the participants’ analysis outcomes to the reference analyses of the “experts,” we did not observe sufficient evidence to support our thesis (see Table 2). Two groups, including the group that did not use the method, produced results that were quite different from the reference analysis (*i.e.*, there was little overlap between the design choices identified by the participants *vs.* those identified by the experts), whereas the third group produced a design similar to the reference design (there was higher degree of overlap). This might also be a function of the available literature and of the type of application at hand.

Table 2 Overlap of participants' design with experts' design

	Group 1	Group 2	Expert	Group 3	Expert
Design Choices relevant to privacy / security	6	8	11	13	13
Overlap with Expert[4]	21%	27%	N/A	53%	N/A

Conclusions

Although it is not possible to infer quantitative conclusions from just three sources of qualitative design process data, this study encouragingly suggests that the proportionality method is usable for its intended purpose. In particular, based on participants' comments and evaluation of the final deliverables, we can draw the following tentative conclusions:

- the method may be particularly fit for exploratory or novel applications, that lack prior deployment history;
- the method may be most useful in case of multiple stakeholders with diverging interests;
- the method may induce designers in evaluating a larger number of design alternatives;
- the method may add little overhead to the design process.
- the application of the method may be useful to talk with stakeholders about the validity of the design choices made (it produced good *rationale* [11]).

We did not gather sufficient evidence to support our second thesis, that the design process can produce repeatable outcomes across experienced and inexperienced designers. However, this study is a pilot of a larger planned study involving up to 70 students, in which we might have enough control to reach a more conclusive answer to this question.

This follow up study will benefit from the experience gained with the present study: we verified the usability of the quantitative metrics for the analysis of the design products; we developed a similarity metric of two designs documents, based on the matching of raised design issues; and we developed a question set for semi-structured interviews.

Acknowledgements

We thank Prof. Seymour Goodman for allowing us to work with his students. We also thank all study participants. Human subjects research is covered under Georgia Institute of Technology IRB approved protocol H05055.

References

1. Bellotti, V., Sellen, A. Design for Privacy in Ubiquitous Computing Environments, *Proc. ECSCW 93*, Kluwer Academic Publishers (1993) 77–92.

[4] Calculated as:
OC / TC
where OC = number of choices on overlapping issues; TC = total number of unique choices (group + expert).

2. Chung, E., Hong J., Lin, J., Prabaker, M., Landay, J., Liu, A. Development and Evaluation of Emerging Design Patterns for Ubiquitous Computing. *Proc. ACM DIS 2004*, ACM Press (2004) 233–242.
3. Hayes, G. Patel, S. Truong, K. Iachello, G. Kientz, J. Farmer, R. Abowd, G.D. The Personal Audio Loop: Designing a Ubiquitous Audio-Based Memory Aid, *Proc. Mobile HCI 2004*, LNCS 3160, Springer Verlag (2004) 168–179.
4. Hayes, G.R., *et al.* Designing Capture Applications to Support the Education of Children with Autism. *Proc. Ubicomp 2004*, LNCS 3205, Springer-Verlag (2004) 161–178.
5. Hong, J., Ng, J.D., Lederer, S., Landay, J.A. Privacy Risk Models for Designing Privacy-Sensitive Ubiquitous Computing Systems. *Proc. DIS 2004*, ACM Press (2004) 91–100.
6. Hong, J., Personal email communication 6/2005.
7. Iachello, G., Abowd, G.D. Privacy and Proportionality: Adapting Legal Evaluation Techniques to Inform Design In Ubiquitous Computing, *Proc. CHI 2005*, ACM Press (2005) 91–100.
8. Jiang, X., Hong, J.I., Landay, J.A. Approximate Information Flows: Socially-Based Modeling of Privacy in Ubiquitous Computing. *Proc. Ubicomp 2002*, LNCS 2498, Springer Verlag (2002) 176–193.
9. Langheinrich, M. Privacy by Design - Principles of Privacy-Aware Ubiquitous Systems, *Proc. Ubicomp 2001*, LNCS 2201, Springer-Verlag (2001) 273–291.
10. Lessig, L. The Architecture of Privacy. *Vanderbilt Journal of Entertainment Law & Practice*, 1, Spring 1999; 1 Vand. J. Ent. L. & Prac. 56.
11. MacLean, A., Young, R.M., Moran, T.P., Design Rationale: The Argument Behind the Artifact, *Proc CHI 89*, ACM Press (1989) 247–252.
12. United States Department of Health, Education and Welfare. *Records, Computers and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (1973).
13. Weiser, M. Some Computer Science Problems in Ubiquitous Computing, *Communications of the ACM*, 36:7, July 1993 (1993) 75–84.